Farrahi and Zia *Hum. Cent. Comput. Inf. Sci.* (2017) 7:4
DOI 10.1186/s13673-016-0085-y

Human-centric Computing and Information Sciences

RESEARCH Open Access

Trust reality-mining: evidencing the role of friendship for trust diffusion

Katayoun Farrahi[1] and Kashif Zia[2*]

*Correspondence:
kzia@soharuni.edu.om
[2] Faculty of Computing and Information Technology, Sohar University, Sohar, Oman
Full list of author information is available at the end of the article

Abstract

Value sensitive design is driven by the motivation of making social and moral values central to the development of ICT systems. Among the most challenging concerns when imparting shared values like accountability, transparency, liberty, fairness and trust into information technology are reliable and comprehensive formal and computational models of those values. This paper, educated by trust theories and models from cognitive science, social sciences and artificial intelligence, proposes a novel stochastic computational model of trust, encapsulating abstractions of human cognitive capabilities and empirically evidenced social interaction patterns. Qualitative and quantitative features of trust are identified, upon which our formal model is phrased. Reality mining methods are used to validate the model based on a real life community dataset. We analyze the time-varying dynamics of the interaction and communication patterns of the community, consider varying types of relationships as well as their symmetry. Social network data analysis shows that our model better fits the evolved friendships compared to a well designed synthetic trust model, which is used as the baseline.

Keywords: Pervasive trust, Socio-technical systems, Value sensitive design, Reality mining

Social interactions and friendship

The diffusion of new ideas, opinions, and relationships are important questions within the social sciences. Even recently, the mechanisms of diffusion of these social behaviors are mostly not understood. Trust is an important concept to understand and model as it influences the behaviors, opinions, and relationships over every social being. It has been studied in the fields of artificial intelligence, economics (game theory) as well as the cognitive sciences. Until recently, there has been no method to automatically capture a community's daily attributes over a long duration and on a fine-grained and multi-modal scale to better model these diffusion processes and more importantly to validate it. In this paper we propose a model of trust which incorporates key features from existing trust models in a manner which can be validated with real-life interactions and communication patterns sensed by mobile phones in a community.

With the aid of ubiquitous sensors and detailed user surveys collected by 80 individuals in an undergraduate student community over the duration of the academic year, we perform a quantitative analysis of a real-life trust diffusion network. We consider the time-varying patterns of close friendships as trusting relationships and additionally

incorporate the true interaction patterns via Bluetooth as well as communication patterns and user beliefs obtained by opinion surveys in validating our work. Using Bluetooth as the communication option is significant as it provides a direct existence of users in a proximity. Our approach extends previous works in several ways, most importantly by using a real-life, long term evaluation and by considering ubiquitous multi-modal sensors for validation.

The contributions of this paper are summarized as follows: first we propose a trust model which generalizes and extends existing trust models by:

- formulating the propagation of trust as a probabilistic stochastic process.
- incorporating features which can be more directly measured and simulating a stochastic process which can be evaluated with real data.
- considering a general formulation which could then be extended and applied to specific applications (as opposed to developing the model for a specific application and goal).
- incorporating various types of interactions directly into the model, and additionally having the flexibility of incorporating transitive interactions (i.e., if A interacts with B which interacts with C, C could be indirectly gaining trust towards A through their mutual friendship with B).

Secondly, we consider a unique and multi-faceted data collection which includes multiple types of mobile phone sensed features over the duration of an academic year, as well as dependent variables regarding participants' relationships and opinions. We compute some statistics and analysis on the social network to show insights into human relationships as well as relationship symmetry. For example we find that over the academic year, the number of symmetric relationships decreases and the number of asymmetric relationships grows. Finally, a case to formally evaluate our trust model has been developed, considering close friendships as trusting relationships. A random model is taken as baseline model for comparison. The topic of interest for trust is the political opinions of individuals, more specifically, their preferred party from which users' beliefs are obtained.

Computational models of trust

Theories of trust in social sciences

It is difficult to settle on a single definition and formalism of trust. Different fields have their own perspective. There are at least three approaches which are followed [1].

1. Decision theoretic approach: in decision making mathematical formulations, the outcome of a decision is not known. The models [2, 3] in this approach use probabilistic or fuzzy theories to evaluate options and designate trust to sources based on the usefulness of previous decisions.
2. Game theoretic approach: game theocratic models are a special case of decision theocratic models. These models [4, 5] perform cost-benefit (or utility) analysis in which the combined benefit of a society of individuals is optimized where individuals expect others to perform actions which benefit them, consequently increasing trust towards them, or vice versa.

3. Socio-cognitive approach: socio-cognitive approaches [6] model mental states that lead to trust (or distrust) and their consequences on modified mental states. These models are implicitly attached with beliefs about the society or the situation and trust is a function of these beliefs [7]. According to [1], the main model in this category is that of Castelfranchi [6] in which trust on an individual is delegated based on previous mutual experiences internally affected by comparative beliefs and related cognitive states.

Most of the computational trust models lie under the decision or game theocratic category. Though these formulations are useful they may not be realistic, particularly in social contexts. The reasons being: (i) humans are not really logical entities and operate under cognitive and social overload rather then empirical reasoning, consequently, (ii) community benefit is not the motive humans are always interested in due to instincts of selfishness and social bias. Additionally, these models do not work in complex scenarios [8] when there is complexity in terms of relations and interactions of individuals. Further, in many situations, either humans are not able to perform a thorough utility analysis due to limited resources (mental capability, fading memory, limited knowledge etc.) or do not have enough time to do that, thus mostly adopting "intelligent" guessing [9] or take risk [10]. In contrast, the socio-cognitive models adopt a completely different approach [11] with their own set of drawbacks. From the perspective of cognitive studies, (i) defining relationships between cognitive processes is a difficult task due to multiple inputs from studies in psychological, neurological and social theories of human behavior, and (ii) models must be abstracted to gain an approximate mathematical formulation. Whereas from the perspective of trust formulations, (i) the related cognitive attributes are diverse and scenario dependent, and (ii) relating social contagion process with a decision making threshold is a difficult task due to variations in human behavior and context.

According to Esfandiari [7], there is no contradiction in both approaches as both treat trust as a variable with a threshold for action with similar characteristics (see Table 1). However to overcome the difficulties mentioned above, it is proposed that a combined approach should be followed [8]. One of the few efforts in this direction is reported in [12]. In this agent-based socio-cognitive model, the decision making is based on affective reasoning abstracted from psychological, neurological and social theories of human behavior. The authors divide the cognitive attributes into two categories, i.e. emotions and intentions. Emotions are mental states of an individual in a situation. The model is scenario specific in which emotions are mental states (hope and fear) relating to panic situation during evacuation. Intentions are goals of the individuals based on their role (commuters and fire-fighters). The decision making model relates utility of information with cognitive overload where an agent takes an action if the cognitive attributes of the deciding agent itself and that of its surrounding points, favor taking an action, where agents can have more trust on one kind of agent (fire-fighters). However the action may not correspond to the action recommended by fire-fighter agents due to cognitive influence of local contradiction. In this way they have modeled decision making under the influence of cognition, combining the above two approaches. However, this model is devised for a specific scenario and works well with it. In other scenarios, the

requirements can be different. For example in our stochastic model of trust for social networks, the consequence of action is not required to be communicated as it is irrelevant. Similarly cognitive attributes are not modeled and remain irrelevant. The motivation of our model is inherited from the notion of belief in [12] for decision making while still adhering to common aspects of trust formulations, when relevant (see Table 1).

Pervasive sensing for human interaction networks

Human interactions in the real world present a great avenue for understanding user behavior. Long term monitoring has been implemented using electronic badges as sensors [13–16] and later mobile phones as sensors [17–21].

The movement to model face-to-face interactions in social networks using sensing technology began with the work of Choudhury and Pentland [22] who devised the sociometer to understand the network structure, and detect when people were in conversation. Olguin el al extended the use of the sociometer by introducing sociometric badges capable of sensing multiple types of features with the goal of understanding how patterns of human behavior shape individuals and organizations [16]. Choudhury and Basu [14] modeled turn-taking behavior in face-to-face conversations and found that participant influence in joint turn-taking was correlated with betweeness centrality.

Mobile phones, carried by billions worldwide on a continuous basis, have also been recognized as potential ubiquitous sensors of location, proximity, and communication, termed Reality Mining [18]. Mobile phone sensors were first used to learn the network

Table 1 Classification dimensions

Model	Modeling approach	Interaction	Visibility	Information in context	Agents behavior	Information transitivity	Reliability measure	Cognitive aspects
Alexei [12]	DSC	DI, SI	S	✓	n/a	n/a	x	MB
Castelfranchi [6]	SC	Not clear	S	✓	x	n/a	x	B
Esfandiary [7]	DT	DO, DI, TI	S	✓	x	x	x	B
Marsh [3]	DT	DI	S	✓	x	n/a	x	n/a
Rahman [2]	DT	DI, TI	S	✓	✓	✓	x	n/a
ReGreT [30]	DT	DI, TI, SI,	S	✓	✓	x	✓	n/a
Yu [31]	GT	DI, TI	S	x	x	x	x	n/a
Our model	DT	DI, TI, SI	S	✓	n/a	Possible	x	B

Modeling approach: Decision-theoretic (DT), game-theoretic (GT), socio-cognitive (SC), combined DT-SC approach (DSC)

Interaction: The type, extent and mode of information sharing between individuals

Sub-categories: Direct Interaction (DI): Directly interacting with others, Direct Observation (DO): Observing interactions of others, Transitive Interaction (TI): Making use of indirect information, Sociological Interaction (SI): Making use of social information including bias towards certain individual types

Visibility: Trust information is available Globally (G) or is local and Subjective (S)

Information in context: Whether information is seen in Context (✓) or not (x). Context can be the topic in which an individual is operating

Agents behavior: Handles the existence of malicious individuals (✓), or not (x), otherwise n/a

Information transitivity: In case of transitive interaction, how the information is exchanged (✓ for different options), no exchange (x), otherwise (n/a)

Reliability measure: Does the model use a trust reliability measure (✓) or not (x)

Cognitive aspects: Does the model include cognitive aspects in decision making, only beliefs (B), both mental states and beliefs (MB) or not (n/a)

structure in a community at MIT [18]. Gonzalez et al [23] have shown that call detail records can be used to characterize temporal and spatial regularity in human mobility patterns. Other examples of the use of mobile phones to map human interaction networks include the CENS participatory sensing project [17], the Darwin project [20], analysis based on machine learning methods [19], and dynamical network theory [21].

Modeling the dynamics of trust

Referring to Table 1, the model described next is strictly mathematical and decision theoretic incorporating important aspects of belief in the trust calculation, thus avoiding the unnecessary burden (not required in current scenario) of understanding and modeling the underlying cognitive attributes. The model considers direct interactions and sociological interactions (as biases) and has the flexibility of additionally representing transitive interactions. The visibility of the model is only subjectively represented by evidential links which can be local (proximity based) as well as space independent. In addition, it supports variations in individual as well as situational context. The capability of individuals to slowly forget (the diminishing memory factor), a feature ignored by most trust models, is also considered by our model. In summary, the model features most of the common features found in trust formulations in a simplistic fashion suitable to general scenarios. At the same time it is flexible enough to be extended and represents a very specific scenario.

Let us consider a population of N individuals whose connections to each other form a graph. We consider two types of links between users, interactions and trust, defined in more detail below. Considering M topics and C categories for each topic, then each person has a set of beliefs about each topic m, $B_i = [B_{c,m}]_{C\times M}$. A person can have a degree of belief in more than one category such that $\sum_c B_{c,m} = 1$ and $B_{c,m} \in [0, 1]$. For simplicity, we consider a single topic m in the model formulation. The formulation can then be extended for all of the M topics of interest by assuming the process behaves the same for all m.

The following link types are modeled.

- Interactions: The first type of dynamic link connecting nodes are the interaction patterns between people, denoted by K. Direct interactions can include face-to-face, phone calls, and email communication. There exists indirect types of interactions as well, an example is information passed through mutual friends. These types of secondary interactions can also be represented by K. Interactions can be measured in different ways, frequencies, durations, or events. In our analysis, we consider numbers of events as this is directly the output from the sensors and involves the least amount of processing and data manipulation. Interactions can be directed or undirected. In the case of phone communication, for example, there are incoming and outgoing phone calls. We consider undirected links, however, in order to more readily combine multiple types of sensor data as K since Bluetooth interactions are undirected. $K = [K_{i,j}]_{N\times N}$ where for a given time $K_{i,j} \in [0, 1]$ and $\sum_j K_{i,j} = 1$, for all $1 <= i <= N$ since K_i is normalized over each user i's total interactions. We use the notation K_I to represent Bluetooth interactions and K_C to represent phone interactions.

- Trust: The second type of dynamic link connecting nodes is trust, denoted by $T.T = [T_{i,j}]_{N\times N}$ where $T_{i,j} \in [0,1]$ and represents a degree of trust between a pair of individuals. $T_{i,j}$ is a directed link indicating there is a trust from i to j, $T_{i,j}$ is the degree of trust i has for j. The change in trust over time is defined as follows,

$$T_{i,j}(t) = T_{i,j}(t-1) + \Delta T_{i,j} \tag{1}$$

where the initial trust person i has for j is $T_{i,j}(0)$.

Other features of the model are given below.

- Similarity in belief: $S_{i,j}$ is a similarity in belief measure. People with similar beliefs tend to have more trust with each other than people with vastly differing beliefs.

$$S_{i,j} = 1 - |\sum_{c} B_{c,i} - B_{c,j}| \quad where\, 0 <= |B_i - B_j| <= 1. \tag{2}$$

If $|B_i - B_j| = 0$, i and j have identical beliefs and the similarity in beliefs becomes maximum $S_{i,j} = 1$. If $|B_i - B_j| = 1$, i and j have opposing beliefs and $S_{i,j} = 0$.

- Influence factor: $\alpha_{i,j}$ is a bias i has towards j, which could be due to many factors. $\alpha = [\alpha_{i,j}]_{N\times N}$ and $\alpha_{i,j} \in [0,1]$. For example people may be more influenced by individuals of a certain sex, class, or appearance.
- Memory factor: β is a constant factor mimicking the effects of memory over time. Basically, the effects of trust are diminished over time without interaction due to memory. This is modeled as a constant β here. It could vary over individuals, some people have better memory than others, but we set it as a constant for simplicity.
- Change in trust: The change in trust person i has towards j, $\Delta T_{i,j}$ is defined as a probabilistic measure. Given users i and j interact $K_{i,j}$ times and have a similarity in beliefs $S_{i,j}$, there is a probability

$$p_{i,j} = \alpha_{i,j} * K_{i,j} * S_{i,j} - \beta \tag{3}$$

that user i will change their trust for user j. Thus the greater the number of interactions, the larger the probability the user changes their trust. At time t, the probability user i changes their trust given their interactions and beliefs is the probability of $(t-1)$ failures to change trust $(1 - p_{i,j})$, times the probability of changing trust at time t, given by $p_{i,j}$. Thus,

$$p(\Delta T_{i,j}(t)) = p_{i,j} * (1 - p_{i,j})^{(t-1)} \tag{4}$$

The trust model is simulated stochastically and the algorithm is shown in Fig. 1. The process is simulated using an event-driven scheme where we draw the time t at which the next person's trust in someone changes given they have interacted. We assume the probability an individual changes their trust in an individual with which they have interacted is given by a geometric distribution. Time is sampled for every pair of interacting users from the distribution in Eq. 4. The user pair i, j with the minimum time sampled is the first to have a change in trust occur between them. That trust $T_{i,j}$ is updated by the relation given in step 10 of Fig. 1 and the trust for the rest of the users remains unchanged. The results should be averaged over a large number of random trials. We set the time bin (used in Step 8 of Fig. 1) to $\delta t = 10^{-6}$ for all simulations. We now introduce the real data collection which we use as one example to validate this model in "Trust diffusion in a real-life social network" section.

// GOAL: Given a topic m and a community of size N with model parameters α, β, S, $T(0)$, and K, estimate the trust i has for j over time $T_{i,j}(t)$.

// Initialization
1) Initialize the parameters, $T_{i,j}(0)$ for all $1 <= i <= N$ and $1 <= j <= N$.
2) Set β.
3) Set each element $\alpha_{i,j}$ in the matrix $[\alpha_{i,j}]_{N\times N}$.
4) Formulate a matrix of beliefs for each individual B_i.
5) For each pair of individuals, form a similarity in beliefs matrix $S_{i,j}$ where $S_{i,j} = 1 - |\sum_c B_{c,i} - B_{c,j}|$.
6) Set appropriate parameters for convergence (e.g., $NN = 0$ or $t_{total} = 200$)

// Run the stochastic process
7) **Iterate** until a convergence condition is met
(e.g. while $t < t_{total}$ or while number of new trusts formed $< NN$ where NN is the total number of new trusts accumulated over time):
8) **Sample** $N \times N$ times $[t]_{N\times N}$ from the distribution:
$p(\Delta T_{i,j}(t)) = \alpha * K_{i,j} * S_{i,j} * \delta t - \beta * \delta t * (1 - \alpha * K_{i,j} * S_{i,j} * \delta t - \beta * \delta t)^{t-1}$
9) Select the minimum time completed from $[t]$, $t_{i,j}^{min}$.
10) Change the trust of user i towards user j by $\Delta T_{i,j}$ such that
$T_{i,j}(t + t_{i,j}^{min}) = T_{i,j}(t) + \Delta T_{i,j} where \Delta T_{i,j} = \alpha * K_{i,j} * S_{i,j} - \beta$
11) If using NN as convergence, compute the number of new accumulated trusts NN. Consider if $T_{i,j}(t + t_{i,j}^{min}) > 0 and T_{i,j}(t) = 0$ then $NN = NN + 1$.
12) Set $t = t + t_{i,j}^{min}$.

Fig. 1 Stochastic process for the diffusion of trust in a network

Trust reality mining

Mobile sensing platform

The approach used in this paper is to pervasively sense the actions of a community over a long period of time using mobile phones. This approach has several advantages considering our overall goal to understand the trust diffusion in a community. We are able to capture multiple types of sensor data including location, interaction, communication, and dependent training labels. Secondly, from a privacy perspective, this requires the user's explicit participation in data collection. Additionally, the community chosen is a tightly knit community and the campaign started at the beginning of the academic semester, throughout which relationships develop. On the other hand, deploying an experimental platform within a community is limited by scale, cost, and effort.

The data was collected for the purpose of measuring the shifts in individual habits, opinions, health, and friendships. Here we present an extension of the dataset, which has previously been analyzed [24–26], and apply it for modeling trust. In this paper, we consider the entire academic year consisting of 270 days, previous works consider only 3 or 4 month durations of data. We are also considering relationships between the individuals in addition to the other features.

Given the above goals, the mobile phone based platform for data-collection was designed with the following long-term continuous sensing capabilities, using Windows Mobile 6.x devices. Daily captured mobile sensing data was stored on-device on read/write SD Card memory. On the server side, these logs files were merged, parsed and

synced by an extensive Python post-processing infrastructure, and stored in MySQL for analysis. This sensing software platform for Windows Mobile 6.x has been released under the LGPLv3 open source license for public use [27]. An important concern with long-term user data collection is securing personal privacy for the participants. This study was approved by the Institutional Review Board (IRB).

The software scans for Bluetooth wireless devices in proximity every 6 minutes. The Windows Mobile phones used in our experiment were equipped with class 2 Bluetooth radio transceivers, with practical indoor sensing range of approximately 10 feet. Scan results for two devices in proximity have a high likelihood of being asymmetric which is accounted for in our analysis by assuming symmetry and undirected links.

The software logged call and SMS details on the device every 20 minutes, including information about missed calls and calls not completed.

Dataset characteristics

The experiment was designed as a long-term longitudinal study with eighty residents of an undergraduate residence hall that served as the primary residential, cooking, social activity, and sleeping quarters for the residents. The participants in the study represent 80 % of the total population of this hall, and most of the remaining twenty percent were spatially isolated. The students were distributed roughly equally across all 4 academic years (freshman, sophomores, juniors, seniors), about 54% were male and predominantly engineering, mathematics and science majors. The study participants also included four graduate resident tutors that supervised each floor.

During the 2009 academic year, the dataset consists of 270 days, 3.15 million scanned Bluetooth devices, 61,100 logged call data records, and 47,700 logged SMS messages. Of these 2.08 million scanned Bluetooth devices belong to other experiment participants, and 11,289 calls and 9533 SMS messages are exchanged with other experiment participants. The following dependent variables were also gathered through surveys.

- Relationships: For each monthly survey, participants identified other residents that were their close friends, political discussants, social acquaintances, and whether they shared facebook and blog information, identical to those used in [28].
- Political opinions: The political opinions were captured using 3 monthly web-based surveys, once each in September, October, and November 2008 (immediately following the presidential election). The monthly survey instrument was based on established political science literature, and consisted of questions shown in [25]. The question we consider in this paper is the user's political party preference. The possible responses for the question were {Democrat, Republican, Independent, or Other}. Political scientists have established that shifts in political opinions are gradual [29]. This is observed in our dataset, as approximately 30% of the 67 participants changed their opinions for each of the dependent questions during the 3 month observation period. Opinion changes were along 1-point or 2-points on the respective 4/7-point Likert scales. Similar variations to dependent variables were also reported in the analysis of Lazer and Rubineau [28].

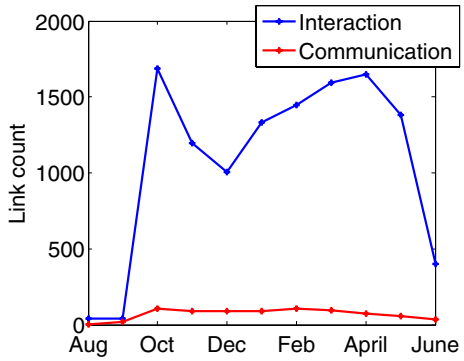


Fig. 2 Link count for the interaction and communication networks. Number of pairs whom interacted at least once within the duration of the month. The monthly communication network is mostly constant over time in comparison to the Bluetooth network. The interaction network shows most of the data collection occurred between October to June, which is the mobile sensed data interval chosen for experiments

Analysis

Sensor-based social network

Considering an interaction network where the users are represented by nodes and interactions are represented by links between nodes, then we can compute the number of links in the network for both the Bluetooth interaction and phone communication of the real data collected. We assume undirected networks and the number of events occurring over a duration of 1 month. Figure 2 shows the link count of the data over time. We can see a jump in links at October, which is when most of the users started using the devices. There is a decrease in the Bluetooth interactions in December, due to the exam period and Christmas holidays. The phone communication however is mostly constant over time.

For each person in the study, we compute the number of people they interacted with as well as called, the number of people they called but never met with in person, and the number of people they interacted with but never called and display the statistics in Fig. 3. There were about 30 people who called another individual in the study but never were in physical proximity to them. As expected, many users were in proximity with each other but never called one another. These figures show that by considering K_I, we capture the bulk of the interacting pairs, as there are few pairs who called one another without ever being in physical proximity.

Survey-based social network

Now we consider a modified network from "Sensor-based social network" section, such that users are represented by nodes however links represent relationships between users. We can then count the number of links over time for the five types of relationships asked in the questionnaires from "Dataset characteristics" section. These relationships are, close friendships, socialize, political discussants, share facebook photos, and share blog information. In Fig. 4 we consider an undirected network where symmetric ties are counted as 1 link and asymmetric ties are also counted as 1 link. We can see there are fewer overall close friendships and political discussants perhaps due to being more personal in nature. There are fewer close friendships than other relationships, and

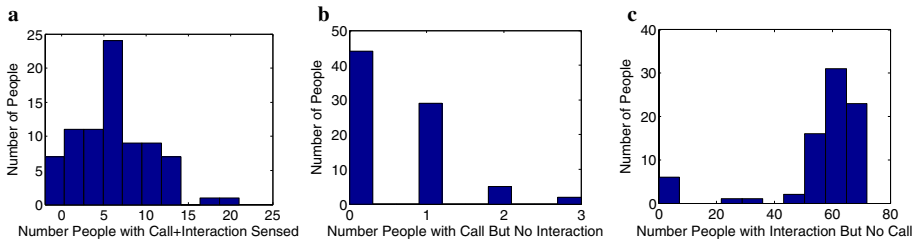


Fig. 3 The distribution of the number of people users (**a**) both called and were in proximity with, (**b**) called but were never in proximity with, (**c**) were in proximity with but never called

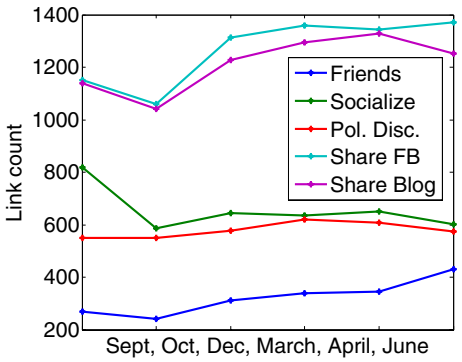


Fig. 4 Friendship link count over time for five types of relationships, friends, socialize, political discussants, share facebook, share blog. Close friendships are probably the most personal relationship with the fewest links. Sharing facebook details has the most number of links at all times. All relationship types increased throughout the school semester, except for socialize, which decreased

this relationship involves the most amount of trust between individuals. We use close friendships in "Trust diffusion in a real-life social network" section as a measure of trust between individuals to perform a validation of our model. There are more pairs of individuals that share facebook information than other types of relationships. We now look more closely at the symmetry between these links.

We consider the distribution of the average monthly interactions, K_I and K_C in Fig. 5 for the four categories (a) never symmetric friends (b) maintained symmetric friends (c) new symmetric friendships and (d) lost symmetric friendships. We are considering the first and last month of the semester. What we mean by 'new symmetric friends', for example, in September user A did not select user B as a close friend, and vice versa for user B and user A. However in June, both user A and B selected each other as close friends. This logic is used for all categories. In the four categories shown in Fig. 5, the top plot is K_I and the bottom plot is K_C. We can see from (a) that users who were never symmetric friends had mostly no interactions and call activity, which is not surprising. The two categories (b) and (c) had a wide range of average monthly interactions. There were several users who maintained friendships with very large amounts of monthly phone activity. This was not observed in the new symmetric friends category, where on average the monthly number of calls was less than 10. Users that lost symmetric friendships also typically had few monthly interactions and phone calls with a few exceptions.

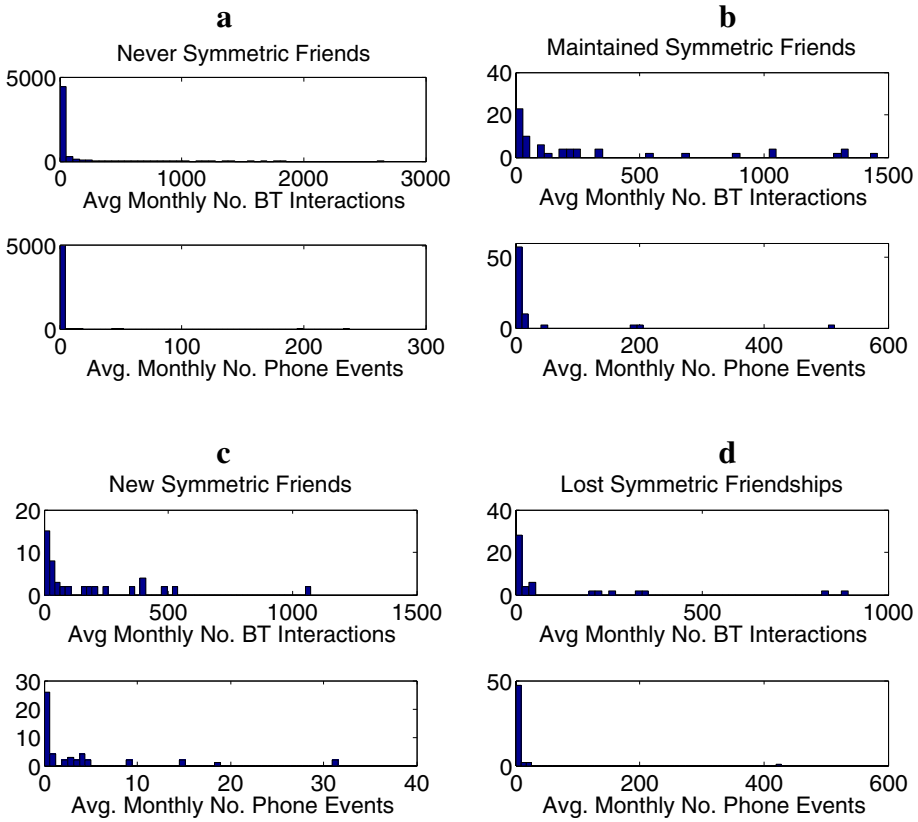


Fig. 5 The distribution of K_I and K_C considering symmetric links for (**a**) never friends (**b**) maintained friends (**c**) new friends and (**d**) lost friends. The friendship changes are considered over the entire academic year (Sept–June). Maintained and new symmetric friends had the most number of average monthly Bluetooth interactions as well as call activity

In Fig. 6, we show a summary of the number of symmetric and asymmetric links for all five relationships for (a) the first and (b) last month of the academic year. Over time the number of symmetric links is decreased for the various types of relationships and the number of asymmetric links increases for almost all types of relationships (except socialize). In Fig. 6 (c) we plot the users' close friendship statistics in terms of the number of asymmetric (non-reciprocated) links as a function of number of symmetric links for September. We can see some users have no symmetric friendships ($x = 0$) and some have entirely symmetric friendships ($y = 0$).

Trust diffusion in a real-life social network

Sensor-based features for modeling

The model parameters taken from the real data are N, $T(0)$, S, K, and the number of new friendships gained over the duration of the study, NN, which is used as a convergence measure in validating simulations. Close friendships are considered to be trusting relationships. The first month of data available on friendships is used as a starting point for the model; data from September is used for model initialization. The last month of available data on friendships, June, is used for validation. Other real data features used are as follows.

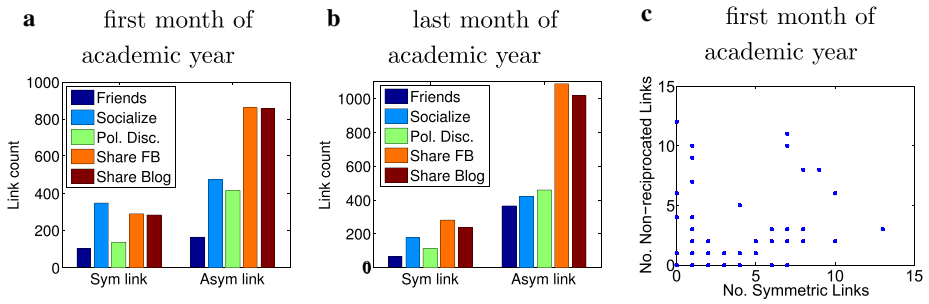
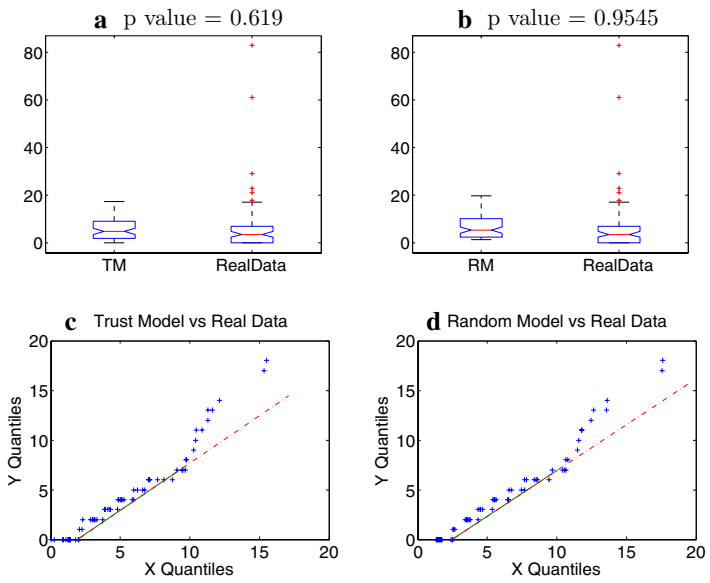


Fig. 6 Number of symmetric and asymmetric links for the five types of relationships for (**a**) September and (**b**) June. Overall, over the course of the academic year, the number of symmetric links decreased and the number of asymmetric links increased for most of the relationship types. In (**c**) we plot the user statistics for close friends were each data point is a user plot in terms of his/her number of asymmetric (non-reciprocated) links as a function of number of symmetric links. We can see some users only had asymmetric friendships, whereas some users only had symmetric friendships

- N is the number of individuals modeled by the stochastic process. Since the maximum number of users with data for both survey questions and mobile phone log features is 80, we set $N = 80$.
- $T(0)$ is the initial $N \times N$ trust matrix, where $T_{i,j}(0) = 0$ if there is no initial trust between users i and j, and $T_{i,j}(0) > 0$ if there exists some degree of trust between users i and j initially. The number of initial close friendships per user is used to initialize $T_i(0)$. The set of users j to which user i has trusted relationships, however, is sampled randomly. Also, if $T_{i,j} > 0$, then we set $T_{i,j} = 0.1$.
- $K_{i,j}$ is a measure of the amount of interaction between a pair of users. We consider three forms of interactions from the mobile sensor data, (1) the Bluetooth interaction data, K_I, (2) the phone communication logs including both call and SMS activity, K_C, and (3) the total combined mobile sensed interaction data, $K_I + K_C$. The total number of events logged by each type of sensor between the pair of users is accumulated over the duration of the study, and normalized such that $\sum_j K_{i,j} = 1$. We consider a constant matrix K_I, K_C, or $K_I + K_C$ over time.
- S is the similarity in opinion between users. We use the real survey responses to the political opinion questionnaire to formulate B from which S is obtained using Eq. 2. We consider the preferred party topic on a 4-point Likert scale, where the possible categories are {democrat, republican, independent, other}. In this case, a user can have only belief for one category due to the nature of the questionnaire given, thus either users have similar beliefs, $S_{i,j} = 1$, or differing beliefs $S_{i,j} = 0$.
- NN is the number of new close friendships formed during the data collection campaign throughout the year. We exclude self-reported friendships (which occur in a few cases) and take into account the symmetry of the data. $NN = 126$ in this case.

Friendship as a measure of trust

We compare the distribution of trust obtained by our trust model (TM), to the actual distribution of close friendships developed over time. The trust model, also abbreviated as 'TM' in the figures, is our proposed trust model. The random model, also abbreviated as 'RM', is a random model where the trusts are diffused randomly to NN members of the community, given real friendships for initialization.



e

	$K_I + K_C$ Trust Model	$K_I + K_C$ Random Model
Symmetric K-L Divergence	**2.0508**	2.1507
Earth Mover's Distance	**0.2319**	0.275
Q-Q plot slope	**0.9756**	0.9211

Fig. 7 Simulation results for $\alpha = 0.1$ and $\beta = 0.1$ for K_I and K_C. Figure **a** and **b** show the f-test results for the distributions of (**a**) our trust model (TM) versus the real data and (**b**) a random model (RM) versus the read data. In both cases p is large indicating the model distributions are adequately fitting the data and are not statistically significantly different. Note, the same experiments with friendship replaced by political discussants produced statistically significantly differing fits. The quantile-quantile (QQ plot) for (**c**) the TM versus the real data and (**d**) the RM versus the real data. The better the distribution fits the real data, the more the slope approaches 1. The slopes are shown in Table (**e**), along with other measures comparing the distributions. Considering all 3 measures, our trust model better fits the real data at the end of the academic year (June 2009) in comparison to a well performing random model used as a baseline

In Fig. 7 we show the simulation results, averaged over 100 random processes for a fixed α and β. We consider several different measures for comparing distributions and in all cases our trust model better fits the real data than the random model. In Fig. 7a, b we show t-test results indicating that the results do not have statistically significantly different distributions than the real data since the p values are greater than 0.05. The random model also closely fits the real data with a large p-value showing it is a competitive model fitting the data decently well. Note, the same experiments with friendship replaced by political discussants produce statistically significantly differing fits. Figure 7c, d fits both models to the real data with a quantile-quantile plot (QQ plot). The closer the results fit the real data, the better the data should fit a linear curve with a slope of 1. The values of the slope are shown in the table below (e) where the trust model's slope is closer to 1. We also compare the distributions in terms of the symmetric Kullback–Leibler divergence (K–L divergence) and the Earth Mover's Distance, two other measures which compute the 'distance' between two distributions. The smaller the distance in both measures, the smaller the distance between the distributions and the better the fit. In both cases the trust model has a lower distance indicating it better fits the real data. These results are

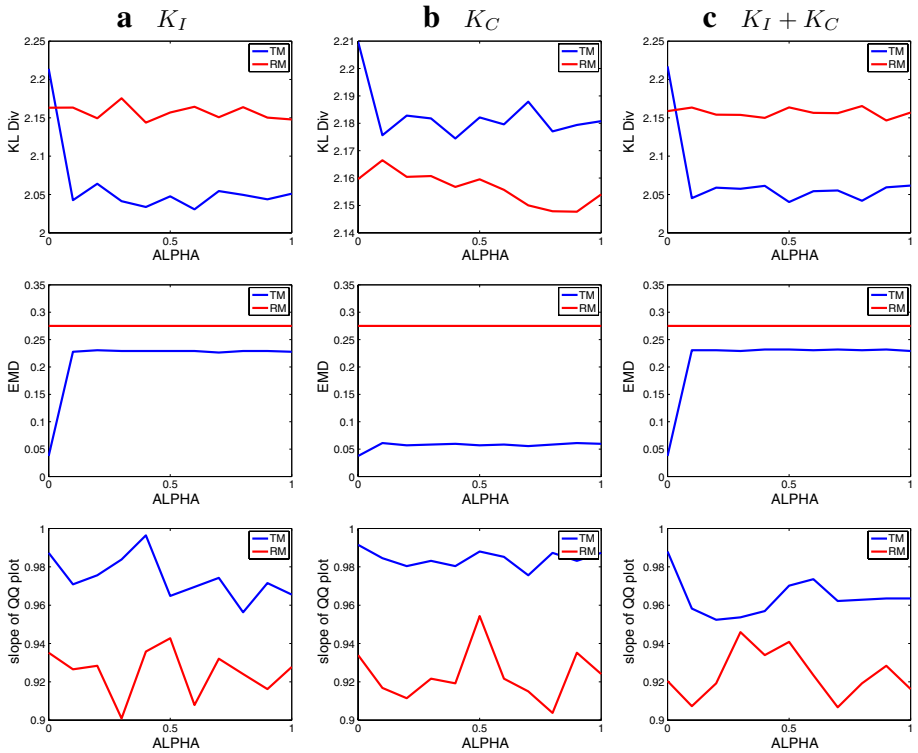


Fig. 8 Results of our trust model evaluated on the close friendship network. Comparison of the performance of our trust model (TM) to that of a random model (RM) in approximating the true evolving nature of the friendship network over time. We compare the distributions in terms of three measures, (*row 1*) the Kullback–Leibler divergence (KL Div) (*row 2*) the Earth mover's distance (EMD) and (*row 3*) the slope of the Quantile–Quantile–Plot (QQ plot). All results are averaged over 100 random trials of the stochastic process. In all cases except for (**b**), our TM for both (**a**) and (**c**) outperforms the baseline

for fixed model parameters and for the case where $K = K_I + K_C$. In Fig. 8 we show the more general results for varying parameters and all cases of K.

Figure 8 compares the difference between our trust model and the real data versus a baseline of the difference between the distributions of a random model and the real data for varying model parameter α, $\beta = 0.1$, and (a) the Bluetooth interaction data (b) the phone communication data and (c) the combination of both. The first row of plots shows the results in terms of the K-L divergence, where the lower the value, the more closely the distribution fits the target. For the Bluetooth interaction, our trust model outperforms the random model for almost all values of α. The random model however outperforms our trust model in terms of the K-L divergence measure for the case of call data only. However, when considering other two measures for comparing distributions (EMD and slope of QQ plot), our trust model outperforms the random model. In every other case considering all other measures, our trust model performs better than the baseline.

Conclusion

The understanding of trust and the mechanisms whereby trust spreads is a phenomenon affecting all social beings which can bring insight to many topics in the social sciences. Trust is important to everyone, it is the foundation from which our society and social

relationships are built. Trust theories and models have been proposed in fields such as artificial intelligence and economics, however proper model validation has always been an issue. Reality Mining has proven to be an effective way of automatically capturing large-scale, fine-grained, time-varying details about humans in a community, providing an invaluable tool for validating such models. In this paper we propose a new model of trust, which uses features presented in previous trust models. Our general and stochastically formulated trust model, encapsulates human features which can additionally be pervasively sensed. We consider a real-life dataset from an undergraduate community collected over an academic year, throughout which relationships are forming and evolving. We analyze the time-varying dynamics of the interaction and communication patterns of the community and further evaluate our trust model on the real data. By using close friendships as a measure of trust between individuals we show that our model better fits the evolved friendships compared to a random model, which is used as the baseline.

Though this analysis has been performed on one community, this work opens questions on how it would apply to other datasets in larger populations and differing communities. The main direction for future extensions of this work would be to explore aspects relating to the data and for additional validation. The model could be evaluated against other types of social networks, new forms of sensor data, over various communities. Additionally, different instantiations of the model parameters, such as the belief parameter, and the interaction parameter, could be explored in further detail. This work, however, provides an initial foundation for trust diffusion modeling based on real world interactions.

Authors' contributions

The authors declare that their contribution is equal in research and preparation of this paper. Both authors read and approved the final manuscript.

Author details

[1] Department of Computing, Goldsmiths, University of London, London, UK. [2] Faculty of Computing and Information Technology, Sohar University, Sohar, Oman.

Competing interests

The authors declare that they have no competing interests.

Received: 11 May 2016 Accepted: 24 December 2016
Published online: 05 February 2017

References

1. Griffiths N, Sarah N, Choi KL (2010) Trust and reputation. Agent-based service-oriented computing. Springer, London, pp 189–224
2. Abdul-Rahman A, Hailes S (2000) Supporting trust in virtual communities. In HICSS. Maui
3. Stephen M (1994) Formalising trust as a computational concept. PhD thesis, University of Stirling, Scotland
4. Schillo PFM, Rovatsos M (2000) Using trust for detecting deceitful agents in artificial societies. Appl Artif Intell 14(8):825–848
5. Wu D, Sun Y (2001) The emergence of trust in multi-agent bidding: a computational approach. In HICSS. Maui
6. Castelfranchi C, Falcone R (1998) Principles of trust for mas: cognitive anatomy, social importance, and quantification. In ICMAS, pp 72–79
7. Esfandiari B, Chandrasekharan S (2001) On how agent makes friends: mechanisms for trust acquisition. In Proceedings of the fourth workshop on deception, fraud and trust in agent societies, Montreal, pp 27–34
8. Jordi Sabater CS (2005) Review on computational trust and reputation models. Artif Intell Rev 24(1):33–60
9. Good D (2000) Individuals, interpersonal relations, and trust. Trust: making and breaking cooperative relations, Department of Sociology, University of Oxford, pp 31–48
10. Luhmann N, Poggi G (1979) Trust and power. Wiley, Hoboken
11. Hesslow G (2002) Conscious thought as simulation of behaviour and perception. Trends Cog Sci 6:242–247

12. Sharpanskykh A, Zia K (2011) Grouping behaviour in ami-enabled crowd evacuation. In ISAmI, vol 92, Springer, Berlin, pp 233–240
13. Choudhury T (2004) Characterizing social networks using the sociometer. Association of computational social and organizational science
14. Choudhury T, Basu S (2004) Modeling conversational dynamics as a mixed memory Markov process
15. Olguin Olguin D, Gloor P, Pentland A (2009) Wearable sensors for pervasive healthcare management. PCT Healthcare
16. Olguin Olguin D, Waber B, Kim T, Mohan A, Ara K, Pentland A (2009) Sensible organizations: technology and methodology for automatically measuring organizational behavior. IEEE Transactions on Systems, Man, and Cybernetics-B
17. Abdelzaher T, Anokwa Y, Boda P, Burke J, Estrin D, Guibas L, Kansal A, Madden S, Reich J (2007) Mobiscopes for human spaces. IEEE pervasive computing—mobile and ubiquitous systems, vol 6, no 2
18. Eagle N, Pentland A, Lazer D (2009) Inferring social network structure using mobile phone data. PNAS 106(36):15274–15278
19. Farrahi K, Gatica-Perez D (2010) Probabilistic mining of socio-geographic routines from mobile phone data. IEEE J Sel Top Signal Process 4:746–755
20. Miluzzo E, Cornelius CT, Ramaswamy A, Choudhury T, Liu Z, Campbell AT (2010) Darwin phones: the evolution of sensing and inference on mobile phones. Mobisys, pp 5–20
21. Onnela JP, Saramäki J, Hyvönen J, Szabó G, Lazer D, Kaski K, Kertész J, Barabási AL (2007) Structure and tie strengths in mobile communication networks. PNAS 104:7332–7336
22. Choudhury T (2003) Sensing and modeling human networks. PhD thesis, M.I.T.
23. Gonzalez M, Hidalgo C, Barabasi A-L (2008) Understanding individual human mobility patterns. Nature 453:779–782
24. Madan A, Cebrian M, Lazer D, Pentland A (2010) Social sensing to model epidemiological behavior change. In Ubicomp, Copenhagen
25. Madan A, Farrahi K, Gatica-Perez D, Pentland A (2011) Pervasive sensing to model political opinions in face-to-face networks. Pervasive, San Francisco
26. Madan A, Moturu S, Lazer D, Pentland A (2010) Social sensing: obesity, unhealthy eating and exercise in face-to-face networks. In ACM wireless health, San Diego
27. MIT Media Lab. Social evolution project. http://social.media.mit.edu
28. Lazer D, Rubineau B, Katz N, Chetkovich C, Neblo MA (2008) Networks and political attitudes: structure, influence, and co-evolution. Working paper series
29. Huckfeldt R, Sprague J (1991) Discussant effects on vote choice: intimacy, structure and interdependence. J Polit 53:122–158
30. Sabater J, Sierra C (2001) Social regret, a reputation model based on social relations. SIGecom Exch 3(1):44–56
31. Yu B, Singh MP (2002) An evidential model of distributed reputation management. In AAMAS, ACM, New York, pp 294–301